Notice of Allowability	**Application No.** 10/086,203	**Applicant(s)** AINSWORTH ET AL.	
	Examiner Ali S. Abyaneh	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *4/3/06*.

2. ☒ The allowed claim(s) is/are *1,2,4-8,11-14,16,22-24,28,30-34,36 and 38-50*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE “MAILING DATE” of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as “replacement sheets”) must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

1. The application has been amended as follows:

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Peter Shaddock on 06-20-2006.

Claims 17, 18, 20, 21 and 37 have been cancelled.

Applicant's attorney was informed of existence of a double patenting between the instant application 10086,203 and pending application 09993132 on 06-23-2006. Applicant has filed a terminal disclaimer to overcome the double patenting.

Allowable Subject Matter

2. Claims 1, 2, 4-8, 11-14, 16, 22-24, 28, 30-34, 36 and 38-50 are allowed.

The following is an examiner's statement of reasons for allowance:

As per claim 1, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: wherein the first receipt information is prevented from being transmitted outside the repository; computing partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; completing the computation of the message digest of the authoritative electronic record, at the remote location, using partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information.

As per claim 16, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: wherein the first receipt information is prevented from being transmitted outside the repository; providing for the computation of a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; providing for transmission of the partially completed message digest of the authoritative electronic record to the remote location; providing for the completion of the computation of the message digest of the authoritative electronic record, at the remote location, using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; providing for the amendment, if the digital signature information is determined to represent a valid digital signature, of the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information.

As per claim 22, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: a method for displaying wherein the first receipt information is prevented from being transmitted outside the repository; computing at the repository a complement of the proper subset of the authoritative electronic record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record.

As per claim 30, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: computing at the repository a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; transmitting to the remote location the partially completed message digest of the authoritative electronic record; allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record.

As per claim 31, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: wherein the first receipt information is prevented from being transmitted outside the repository; wherein the message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information.

As per claim 36, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: wherein the first receipt information is prevented from being transmitted outside the repository; means for transmission to the remote location the partially completed message digest of the authoritative electronic record; means for completing the computation of the message digest of the authoritative electronic record, at the remote location, using partially completed message digest of the authoritative electronic record and complement of the proper subset of the authoritative electronic record; means for amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information.

As per claim 38, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: wherein the first receipt information is prevented from being transmitted outside the repository; computing at a repository a partially completed message digest of the authoritative electronic record, wherein the partially completed message digest is related to the proper subset of the authoritative electronic record; controlling the transmission of the partially completed message digest of the authoritative electronic record to the remote location; allowing the computation of the message digest of the authoritative electronic record to be completed at the remote location; using the partially completed message digest of the authoritative electronic record and the complement of the proper sunset of the authoritative electronic record.

As per claim 39, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: wherein the first receipt information is prevented from being transmitted outside the repository; wherein message digest was computed using a partially completed message digest of the authoritative electronic record and a complement of a proper subset of the authoritative electronic record, wherein the partially completed message digest is related to a proper subset of the authoritative electronic record; amending, if the digital signature information is determined to represent a valid digital signature, the authoritative electronic record to create a signed authoritative electronic record, wherein the signed authoritative electronic record comprises the authoritative electronic record and the digital signature information.

As per claim 40, the prior art Bisbee et al. (US Patent NO 5,748,738) of record teaches authenticating an electronic document comprises the steps of: signing the electronic document with a digital signature of a Transfer Agent; appending a certificate to the electronic document by the Transfer Agent; and validating the digital signature and certificate of the Transfer Agent. The certificate may include information representing the Transfer Agent's identity, public cryptographic key, and predetermined attributes. Bisbee furthermore discloses, the signing step may comprise the steps of applying a hash function to the electronic document to determine a message digest and using the message digest with a secret cryptographic key of the Transfer Agent to determine digital signature. The step of validating the digital signature then comprises the steps of decrypting the message digest with the Transfer Agent's public cryptographic key, applying the hash function to the electronic document to determine a second message digest, and comparing the decrypted message digest to the second message digest (see column 3, lines 1-20).

The prior art Vanstone (US Patent NO 6,212,281) of record teaches generating an encrypted message string, with a key and forwarding the cipher text to a recipient. The encrypted message string is also processed by a hash function and the resulting hash utilized in the signature. The recipient recovers the message by hashing the message string and utilizes the value to recover the encryption key. The message can then be recovered from the message string (see column 2, lines 37-50).

The prior arts taken singly or in combination, fail to anticipate or render the following limitation: computer readable program code devices configured to cause the computer to effect the transmission of a partially completed message digest of the authoritative electronic record, wherein the complement of the proper subset of the authoritative electronic record is a provable representation of the authoritative electronic record, and wherein the partially completed message digest of the authoritative electron in record is related to a proper subset of the authoritative electronic record; wherein the computed message digest is generated using the partially completed message digest of the authoritative electronic record and the complement of the proper subset of the authoritative electronic record; computer readable program code devices configured to cause the computer to effect the amending, if the received digital signature information is determined to be valid, of the authoritative electronic record in the repository to include at least some of the received digital signature information.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh A.A
Patent Examiner
Art Unit 2137
06/22/06

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER